An Update to the Growing Regulatory Risk of Off-Channel and Ephemeral Communications

ADVISORY **Publish Date** June 27, 2023 **By** RANE, Matthew Bernstein C+I LRC

In November 2022, **RANE** published an Advisory on the growing challenges companies face in complying with expanding regulations concerning employees' communications. Since then, there have been multiple developments that warrant an update. The original Advisory referenced a September 2022 speech in which Deputy U.S. Attorney General (DAG) Lisa Monaco announced significant policy changes to the U.S. Department of Justice (DOJ) corporate enforcement strategy, which included an intensified focus on personal device policies and controls and proper document preservation policies and procedures. The policy changes were announced in tandem with a memorandum released the same day, which detailed the changes.

On March 3, 2023, Assistant Attorney General (AAG) Kenneth Polite announced noteworthy revisions to the DOJ's Evaluation of Corporate Compliance Programs (ECCP) guidance. The revisions expand on DAG Monaco's September 2022 comments and introduce new guidance for assessing companies' compliance efforts to monitor employees' use of personal devices and communication platforms. On May 11, federal regulators then illustrated their heightened scrutiny of companies' communications practices by fining two prominent broker-dealers. To review these developments and provide guidance for companies, **RANE** again spoke with **Matthew Bernstein, Founder and Information Governance Strategist at Bernstein Data**.

What to Know:

In a September 15, 2022 speech, DAG Monaco conveyed the DOJ's increasing concern about the prolific use of certain messaging applications — including encrypted and ephemeral messaging applications such as WhatsApp, Signal and Telegram — by company employees for business purposes. The DOJ explicitly noted that these types of communications are often conducted through personal devices rather than company-provided or -monitored programs. The rise in remote work and Bring Your Own Device (BYOD) programs has resulted in an environment that may be inconsistent with an effective compliance program, especially with regard to the potential need to access necessary data and information for audits, reviews or investigations.

In response to these concerns, in March 2023, the DOJ announced revisions to its ECCP to specifically address corporations' approaches to the use of personal devices and messaging applications. Due to the growing prevalence of these messaging applications and corporate BYOD policies, the DOJ now "expects companies to update their policies and practices accordingly." Although the ECCP is intended to guide federal prosecutors, it nevertheless serves as a key reference for organizations, and the DOJ will expect organizations to be familiar with its evaluation criteria. To **Bernstein**, it is clear that the DOJ did not issue the updated evaluation merely as a reminder of the status quo but rather as a pointed notice

about the issues it will be most concerned about going forward.

Then, on May 11, the Bank of Nova Scotia (BNS) and HSBC were fined a total of $22.5 million and $15 million, respectively, by separate U.S. regulators for admitted recordkeeping failures regarding employee use of off-channel communications to conduct company business.

In the first case, the Securities and Exchange Commission (SEC) charged HSBC Securities (USA) Inc. and Scotia Capital (USA) Inc. — a unit of BNS — for widespread and longstanding failures by both firms and their employees to maintain and preserve electronic communications. The SEC's investigation of HSBC Securities and Scotia Capital, both registered broker-dealers, uncovered failings involving employees at multiple authority levels, including supervisors and senior executives. To settle the charges, HSBC and Scotia Capital acknowledged that their conduct violated recordkeeping provisions of federal securities laws and agreed to pay penalties of $15 million and $7.5 million, respectively.

Separately, the Commodity Futures Trading Commission (CFTC) announced a settlement with Scotia Capital for the same conduct, with the brokerage firm agreeing to pay $15 million in fines. In the announcement, CFTC Commissioner Christy Goldsmith Romero provided a statement explaining that the CFTC investigated BNS when it became clear that there were missing communications records. The missing records triggered another investigation where the CFTC "found that most employees regularly used unauthorized communication platforms, with the knowledge and participation of senior leadership. This even included the use of encrypted messaging apps and private texts by those who should have stopped this illegal practice — senior officials responsible for compliance."

Given that this is the third penalty from the CFTC for BNS (following a 2018 enforcement action against BNS for spoofing and a 2020 CFTC enforcement action for spoofing in parallel with a DOJ criminal action), Commissioner Romero made a case for admittance of wrongdoing resolution to more powerfully deter future violations. The commissioner said, "too often, deterrence is only discussed in terms of the size of a penalty (and I support the $22.5 million in combined penalties with the SEC here) ... My experience is that deterrence can be achieved from a defendant having to admit its wrongdoing, combined with a penalty. Particularly defendants with significant resources may view admissions to be more consequential than a penalty."

What to Think About:

Under the new ECCP, prosecutors are advised to "consider a corporation's policies and procedures governing the use of personal devices, communications platforms, and messaging applications, including ephemeral messaging applications." The ECCP states that "[p]olicies governing such applications should be tailored to the corporation's risk profile and specific business needs and ensure that, as appropriate and to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company." The policy encourages prosecutors to "consider how the policies and procedures have been communicated to employees, and whether the corporation has enforced the policies and procedures on a regular and consistent basis in practice."

Bernstein finds the DOJ's emphasis on governance aspects to be particularly interesting. In the past, monitoring of communications was largely subsumed within market surveillance and supervision activities. Efforts to police communications platforms were not as much of a focus. The DOJ is seemingly attempting to bring communications compliance standards and practices into the sphere of traditional compliance using established protocols like employee training, monitoring, and consequences.

Another notable implication of the revised EECP can be found in a statement from AAG Polite, who introduced the ECCP revisions at the American Bar Association (ABA) National Institute on White Collar Crime. As he noted in his ABA speech, should companies decline to provide data from ephemeral messaging applications or other communication platforms, DOJ prosecutors will not accept companies' representations at face value. Rather, they will ask questions about the company's ability to access such communications, whether they are stored on company devices or servers, and whether they have considered and complied with applicable privacy and local laws. "A company's answers — or lack of answers — may very well affect the offer it receives to resolve criminal liability," Polite stated. Polite also clarified that companies with BYOD policies are not exempt from this guidance.

Furthermore, the revised EECP guidance makes clear that the DOJ will assess how organizations implement their data retention policies and the consequences for employees who refuse to grant the company access to their communications. Specifically, the DOJ will look into whether companies discipline employees who fail to comply with the policy and whether the company's approach to managing communication channels — including BYOD — is reasonable in the context of the company's business and risk profile.

Finally, regarding the recent fines against HSBC and Scotia Capital, they are the latest Wall Street companies to face penalties for employees' use of personal devices and messaging apps since regulators launched a broad probe into the use of such platforms in 2021, but they most certainly will not be the last. Both the SEC and the DOJ have made company use of messaging apps a focus of enforcement efforts because of the difficulty they pose to agencies trying to investigate compliance issues. In the past, unless a violation involved fraud or alleged harm to investors, a fine would typically be something less than $1 million, according to an August 2022 report in The Wall Street Journal. The median fine in 2020 was $194,000. But the agencies are using aggressive penalties to make clear that off-channel communications must be off-limits, meaning that financial risks to companies are growing.

What to Consider:

In light of the EECP revisions and the recent penalties on HSBC and Scotia Capital, organizations should expect the DOJ to increasingly and more broadly investigate policies governing the preservation of and access to corporate data and communications stored on personal devices, including data on messaging platforms. To best prepare, organizations can consider the following measures:

- Review existing data privacy and communication policies to see if they need to be updated to reflect DOJ's guidance, as well as identify potential conflicts between local data privacy laws and DOJ guidance and take mitigating steps as appropriate.

- Consider evaluating policies regarding the permissible use of mobile devices and messaging platforms, particularly those relating to BYOD programs. Organizations will no longer be able to avoid the DOJ's preservation and disclosure expectations because employees use their own devices or conduct business on third-party messaging apps that do not preserve data.
- Update training materials to clearly communicate policies to employees and executives and convey incentives and disincentives for compliance; implement mechanisms for compliance monitoring; and enforce consequences for noncompliance.
- Set and practice a culture of compliance at the very top, as regulators are explicit about their displeasure when supervisors and senior executives sanction misconduct by example or inaction.

Bernstein says there is a clear sense that the DOJ expects organizations to be active in their compliance efforts. He suggests that one of the reasons for this emphasis on active governance is the proliferation of novel and evolving communications platforms. Like the SEC before it, the DOJ is broadcasting that it will not accept new technology as an excuse for noncompliance. **Bernstein** says despite the challenges inherent in maintaining situational awareness about all the new, and at times intentionally secretive, communications channels, regulators are ultimately focused on the same types of activities, actions and behaviors they have historically been concerned about. Rather than try to determine how to eliminate the misuse of each individual technology, application, or terminal, compliance professionals should understand how it may enable bad behavior, work to mitigate opportunities for misuse, communicate expectations, incentivize compliance, and follow through on deterrents for noncompliance.

For companies trying to stay abreast of these developing and proliferating types of communications tools, **Bernstein** has three pieces of advice:

- Have a clear policy stating that employees and executives cannot start doing business on a new technology platform, particularly one that enables communication, without informing the compliance department. Whether a mobile application is encrypted or a platform that employees use for business has communication functionality built-in, compliance needs to know how and why employees are using those communication channels. Part of the conversation should include whether the channel is used for convenience or because it is fundamental to doing business in a certain market. Then a determination must be made as to whether communication over that channel can be captured and, if not, evaluate if there is an available compensating control.
- Ascertain how feasible it is to capture communications on new types of communication tools. Bernstein suggests researching companies that specialize in providing communications capture and surveillance services and learning from their research and resources. Then, organizations can understand if they are qualified and capable of communications management internally — for example, by working with developers to build a gateway that intercepts messages and consolidates them in one managed space — or if an external tool, mechanism, or third party is needed.
- Determine whether a BYOD or corporate device policy is appropriate for the company. Bernstein,

who in the initial RANE Advisory said he anticipates a risk-shifting swing from personal devices being used for work back to corporate-provided devices, still maintains that expectation, especially because he noticed an implication in a number of places in the revised ECCP that employees' ability to configure what is captured and retained could be problematic. The update also raises privacy concerns related to the ability to control the personal devices utilized for BYOD.

About the Expert:

Matthew Bernstein led information management practices in various businesses at Deutsche Bank for more than 20 years and now leads his own firm. BernsteinData helps clients implement effective solutions for Information Governance risk and business objectives in Records Management, Information Security, Data Privacy, Legal and Regulatory Responsiveness, and Operational Efficiency. At Deutsche Bank, Matthew was Head of Group Information and Records Management, with global responsibility for Records Management, Archiving, and eDiscovery Operations. Together with the Bank's CISO and CDO, he was responsible for information governance at the bank, which employs more than 100,000 people in over 60 countries.